

**IMPLEMENTASI *PORT KNOCKING* PADA SISTEM KEAMANAN JARINGAN
DENGAN MENERAPKAN ALGORITMA RSA (*RIVEST SHAMIR ADLEMAN*)**

SKRIPSI

Skripsi ini sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika
Universitas Pembangunan Nasional "Veteran" Yogyakarta



Disusun oleh :

I KOMANG HARTAWAN WIJAYA
123060051

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
YOGYAKARTA
2011**

ABSTRAK

Saat ini keamanan telah menjadi hal yang sangat penting, terutama dalam bidang Teknologi Informasi. Statistik tingkat eksploitasi keamanan terhadap banyak *server* dan jaringan makin hari semakin meningkat. Bahkan seseorang yang tidak memiliki pengetahuan yang cukup dalam masalah keamanan jaringan dapat melakukan penetrasi terhadap sebuah sistem jaringan dengan hanya *men-download exploit* untuk sistem yang diserangnya dan kemudian menggunakannya untuk kepentingan sendiri.

Salah satu upaya mengamankan sebuah *server* adalah dengan menggunakan *firewall*, tetapi saat ini *firewall* masih memiliki kelemahan. Sehingga dicari solusi terbaik agar dapat mengakses *service* tertentu walaupun port tersebut tertutup. Metode untuk membuka port tertutup secara eksternal tersebut bernama metode *port knocking*. Metode yang digunakan dalam membangun aplikasi ini adalah dengan Metode *Waterfall*, dengan penyesuaian yang diperlukan untuk membangun aplikasi ini, meliputi rekayasa dan permodelan sistem, analisa kebutuhan, perancangan sistem, implementasi, pengujian, dan pemeliharaan. Dalam pembuatan aplikasi ini menggunakan *Netbeans IDE 2.9.1* dan *CHX packet filter 3.0* sebagai *firewall*.

Berdasarkan hasil analisis dan perancangan, telah berhasil dibuat aplikasi port knocking yang dapat melakukan koneksi ke *server* meskipun port yang dituju tertutup oleh *firewall*. Di dalam uji coba telah berhasil dilakukan akses ke beberapa port *service* yang tertutup seperti port FTP(21), SSH(22), TELNET(23), HTTP(80). Penelitian ini diharapkan dapat membantu administrator untuk mengelola *server* dari *remote area* dan meminimalisir serangan terhadap *server* dengan menyembunyikan *service* yang sedang berjalan pada port tertentu.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN PEMBIMBING	ii
HALAMAN PENGESAHAN PENGUJI	iii
SURAT PERNYATAAN KARYA ASLI SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTTO	vi
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xv
DAFTAR MODUL	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Metode Pengembangan Sistem	3
1.7 Sistematika Penulisan	3
BAB II DASAR TEORI	5
2.1 Sistem	5
2.2 Aplikasi	5
2.3 Jaringan Komputer	6
2.4 Internet	7
2.5 Protokol	7
2.6 Model Referensi Jaringan	8
2.6.1 Model OSI	9
2.6.2 Model DOD (<i>Departement Of Defence</i>)	11
2.7 TCP/IP	12
2.7.1 Model Layanan TCP	14
2.7.2 Manajemen Koneksi TCP	14
2.8 IP Address	15
2.8.1 Kelas-kelas IP Address	17
2.8.1.1 IP kelas A	17
2.8.1.2 IP kelas B	17
2.8.1.3 IP kelas C	18
2.8.2 Pengalokasian IP Address	18
2.9 Port	18
2.9.1 <i>Well Known Port</i>	19
2.9.2 <i>Registered Port</i>	20
2.9.3 <i>Dynamic/PrivatePort</i>	20

2.10 Keamanan Jaringan Komputer dan Firewall.....	20
2.10.1 Bentuk Ancaman Terhadap Jaringan Komputer.....	20
2.10.2 <i>Firewall</i>	21
2.11 <i>Port Knocking</i>	22
2.11.1 Cara Kerja <i>Port Knocking</i>	22
2.11.2 Format Ketukan	26
2.12 Kriptografi.....	29
2.12.1 Pengertian Kriptografi	29
2.12.2 Tujuan Kriptografi	29
2.12.3 Jenis Algoritma Kriptografi	30
2.12.3.1 Kriptografi Simetri (<i>symmetric cryptography</i>)	30
2.12.3.2 Kriptografi Asimetri (<i>asymmetric cryptography</i>).....	31
2.12.4 Algoritma RSA (Rivert-Shamir-Adelman)	32
2.12.4.1 Algoritma Pembangkitan Kunci	32
2.12.4.2 Algoritma Enkripsi	33
2.12.4.3 Algoritma Dekripsi	33
2.12.4.4 Penerapan Algoritma RSA.....	34
2.13 Metode Pengembangan Sistem	35
2.14 Flowchart	36
2.15 Chx 3.0.....	38
2.16 Java	39
2.17 Netbeans.....	39
2.18 Studi Pustaka.....	40
 BAB III ANALISIS DAN PERANCANGAN SISTEM	 41
3.1 Analisis Sistem.....	41
3.1.1 Arsitektur Sistem	42
3.2 Model Analisis	43
3.2.1 Flowchart port knocking dengan menetapkan kriptografi kunci public RSA	44
3.2.2 Flowchart proses pembangkitan kunci (<i>public key</i> dan <i>private key</i>)	46
3.2.3 Flowchart proses enkripsi	47
3.2.4 Flowchart proses dekripsi	49
3.3 Perancangan Antarmuka	51
3.3.1 Perancangan Antarmuka pada <i>Server</i>	51
3.3.1.1 Rancangan Antarmuka <i>Home</i>	51
3.3.1.2 Rancangan Antarmuka Urutan Ketukan	52
3.3.1.3 Rancangan Antarmuka <i>Firewall Setting</i>	53
3.3.1.4 Rancangan Antarmuka About.....	53
3.3.2 Perancangan Antarmuka pada <i>Client</i>	54
 BAB IV IMPLEMENTASI	 55
4.1 Implementasi	55
4.2 Perangkat Keras (Hardware) yang digunakan	55
4.3 Perangkat Keras (Software) yang digunakan	55
4.4 File yang digunakan dalam sistem	56
4.5 Implementasi Sistem dan Interface	57

4.5.1 Implementasi interface halaman knockserver	57
4.5.1.1 Receivethread.....	59
4.5.1.2 Knockthread.....	60
4.5.1.3 OpenData	62
4.5.1.4 ReachableDetectionThread	62
4.5.1.5 RSA.....	63
4.5.1.6 CryptDB.....	64
4.5.1.7 Splitter.....	65
4.5.1.8 Tampilan halaman User Setting.....	65
4.5.1.9 Tampilan halaman Chx Setting.....	66
4.5.1.10 OptionDB.....	68
4.5.1.11 Tampilan halaman About.....	69
4.5.1.12 ImagePanel.....	70
4.5.2 Implementasi interface halaman KnockClient	70
4.6 Implementasi Hasil Uji Coba Ketukan	74
4.6.1 Implementasi hasil uji coba dari client satu	75
4.6.2 Implementasi hasil uji coba dari server	79
4.6.3 Implementasi hasil uji coba dari client kedua.....	81
 BAB V PENUTUP	 84
5.1 Kesimpulan	84
5.2 Saran	84
 DAFTAR PUSTAKA	 85

DAFTAR GAMBAR

Gambar 2.1 Seluruh port ditutup sehingga tidak ada yang dapat mengakses.....	23
Gambar 2.2 Port 22 yang dilindungi dengan metoda <i>port knocking</i>	23
Gambar 2.3 Seorang <i>user</i> melakukan ketukan rahasia	24
Gambar 2.4 Seorang <i>user</i> diizinkan melakukan koneksi.....	25
Gambar 2.5 <i>Flowchart</i> aplikasi <i>port knocking</i>	26
Gambar 2.6 Contoh header dan footer	28
Gambar 2.7 Format ketukan multiple port.....	28
Gambar 2.8 Kriptografi Simetri (<i>symetric cryptography</i>)	31
Gambar 2.9 Kriptografi Asimetri (<i>asymetric cryptography</i>)	32
Gambar 3.1 Arsitektur Sistem.....	43
Gambar 3.2 <i>Flowchart</i> port knocking dengan menerapkan kunci publik RSA	45
Gambar 3.3 <i>Flowchart</i> proses pembangkitan kunci.....	47
Gambar 3.4 <i>Flowchart</i> proses enkripsi	48
Gambar 3.5 <i>Flowchart</i> proses dekripsi	50
Gambar 3.6 Rancangan Antarmuka <i>Home</i>	52
Gambar 3.7 Rancangan Urutan Ketukan	52
Gambar 3.8 Rancangan Antarmuka <i>Firewall Setting</i>	53
Gambar 3.9 Rancangan Antarmuka <i>About</i>	53
Gambar 3.10 Rancangan Antarmuka <i>Client</i>	54
Gambar 4.1 Tampilan form home server.....	57
Gambar 4.2 Tampilan form user setting	66
Gambar 4.3 Tampilan form chx setting	67
Gambar 4.4 Tampilan form open chx log	67
Gambar 4.5 Tampilan form about.....	69
Gambar 4.6 Tampilan form knockclient.....	71
Gambar 4.7 Tampilan scan NMAP sebelum pengetukan	75
Gambar 4.8 Tampilan putty sebelum pengetukan	76
Gambar 4.9 Tampilan proses pengetukan sukses	76
Gambar 4.10 Tampilan proses pengetukan.....	77
Gambar 4.11 Tampilan NMAP setelah pengetukan	78
Gambar 4.12 Tampilan hasil pengetukan port 23	78
Gambar 4.13 Tampilan hasil pengetukan port 80	79
Gambar 4.14 Tampilan urutan ketukan	79
Gambar 4.15 Tampilan pembangkitan public key	80
Gambar 4.16 Tampilan hasil enkripsi	80
Gambar 4.17 Tampilan proses ketukan gagal	82
Gambar 4.18 Tampilan proses ketukan gagal port 80	82
Gambar 4.19 Tampilan scan NMAP.....	83

DAFTAR TABEL

Tabel 2.1 Lapisan (<i>layer</i>) pada model <i>OSI</i>	10
Tabel 2.2 Lapisan (<i>layer</i>) pada model <i>DOD/TCP-IP</i>	11
Tabel 2.3 Perbandingan model <i>OSI</i> dengan model <i>DOD</i>	12
Tabel 2.4 Istilah umum pembentukan komunikasi antar komputer.....	14
Tabel 2.5 Ketukan untuk port tunggal dengan pemetaan tetap.....	27
Tabel 2.6 Simbol-simbol standart pada flowchart program.....	37
Tabel 4.1 Perangkat Keras (Hardware) yang digunakan	55
Tabel 4.2 Perangkat Lunak (Software) yang digunakan.....	56
Tabel 4.3 File halaman Admin.....	56
Tabel 4.4 File dalam halaman Client	57

DAFTAR MODUL

Modul Program 4.1 MainFrame.java.....	58
Modul Program 4.2 Receivethread.java.....	59
Modul Program 4.3 Lanjutan Receivethread.java	60
Modul Program 4.4 Knockthread.java.....	60
Modul Program 4.5 Lanjutan Knockthread.java.....	61
Modul Program 4.6 OpenDatajava	62
Modul Program 4.7 ReachableDetectionThread.java	62
Modul Program 4.8 Lanjutan ReachableDetectionThread.java.....	63
Modul Program 4.9 RSA.java.....	63
Modul Program 4.10 Cryptdbjava	64
Modul Program 4.11 Splitter.java.....	65
Modul Program 4.12 form user setting	66
Modul Program 4.13 form chx setting.....	67
Modul Program 4.14 Lanjutan form chx setting.....	68
Modul Program 4.15 Optiondb.java	68
Modul Program 4.16 Lanjutan Optiondb.java	69
Modul Program 4.17 Form about.....	69
Modul Program 4.18 Lanjutan Form about	70
Modul Program 4.19 Imagepanel.java.....	70
Modul Program 4.20 Form Knockclient	71
Modul Program 4.21 Lanjutan Form Knockclient.....	72
Modul Program 4.22 Lanjutan Form Knockclient.....	73
Modul Program 4.23 Lanjutan Form Knockclient.....	74